RÆSTAD et al
Serial No. 09/655,871

Atty Dkt: 3842-3
Art Unit: 2134

THE CLAIMS:

The following is a listing of pending claims (none of which are amended by this Supplemental Response):

1. (Currently Amended) An arrangement for audio, video, and data communications across packet based networks implementing the H.323 standard recommended by the International Telecommunications Union, the arrangement including one or more gatekeepers, wherein end-user authentication is performed by an authentication proxy.

2. (Currently Amended) An arrangement according to claim 1, wherein a security profile used by the authentication proxy is supported by a gatekeeper associated with said authentication proxy.

3. (Currently Amended) An arrangement according to claim 1, wherein end-user information needed by the authentication proxy is requested from an end-user by a non-proprietary communications protocol.

4. (Currently Amended) An arrangement according to claim 1, wherein the authentication proxy communicates information to a gatekeeper by a H.323 version 2 RAS (Registration, Admission and Signaling) message.

5. (Currently Amended) An arrangement according to claim 3, wherein the non-proprietary communications protocol includes one of http and https.

6. (Currently Amended) An arrangement according to claim 1, wherein information for end-user authentication is provided by an end-user in an html form, an applet, or a servlet.

7. (Previously Presented) An authentication proxy arrangement in a H.323 telecommunication network for allowing authentication of an end-user operating from an H.323 end-point without H.323v2 or H.235 authentication support and with a Gatekeeper requiring initial end-user authentication according to a first authentication protocol using H.235 and thus being unsupported by the end-point, the first authentication protocol being at least part of H.323v2 or a corresponding first security profile, said authentication proxy being adapted to form a signaling path for authentication of the end-point towards the Gatekeeper, the authentication proxy being arranged:

to obtain from the end-point of the end-user, by using a second protocol different from said first protocol, authentication data comprising an end-user password and an end-point network location specification,

to generate a first H.323 RAS (Registration, Admission and Signaling) message using said first protocol, said first H.323 RAS message presenting said obtained authentication data and including an authentication request requesting authentication of the end-user by the Gatekeeper on basis of said presented authentication data,

to transmit said first H.323 RAS message to the Gatekeeper,

to receive a second H.323 RAS message from the Gatekeeper in response to said first H.323 RAS message, to interpret said second H.323 RAS message from the Gatekeeper for detecting a confirmation or rejection of said authentication request, and

to generate and send to said end-point, on detection of said confirmation or rejection of said authentication request, an authentication confirm or reject message, respectively, using the second protocol.

8. (Previously Presented) The arrangement of claim 7, wherein the end-point network location specification is an internet protocol (IP) address or a user name.

9. (Previously Presented) The arrangement of claim 7, wherein obtaining the authentication data is performed by a simple html form, an applet, or a servlet.

10. (Previously Presented) The arrangement of claim 9, wherein the applet is a signed applet.

11. (Previously Presented) The arrangement of claim 7, wherein the second protocol includes http or https.

12. (Previously Presented) The arrangement of claim 7, wherein said first H.323 RAS message is a H.323.V2 GRQ (Gatekeeper request) or a RRQ (Registration request), respectively including H.235 data that includes said authentication data.

13. (Previously Presented) The arrangement of claim 12, wherein the second H.323 message is a GCF (Gatekeeper confirm) or a RCF (Registration confirm).

14. (Previously Presented) The arrangement of claim 7, wherein the authentication proxy is arranged to sending to the end-point of the end-user an http-response indicating authentication failure if the second H.323 message is a GRJ (Gatekeeper reject).

15. (Previously Presented) A method using an authentication proxy arrangement in a H.323 telecommunication network for allowing authentication of an end-user operating from an H.323 end-point (1) without H.323v2 or H.235 authentication support and intending to operate with a Gatekeeper requiring initial end-user authentication according to a first authentication protocol using H.235 and thus being unsupported by the end-point, the first authentication protocol being at least part of H.323v2 or a corresponding first security profile, said authentication proxy being adapted to form a signaling path for authentication of the end-point towards the Gatekeeper, said method including:

obtaining from the end-point of the end-user, by using a second protocol different from said first protocol, authentication data comprising an end-user password and an end-point network location specification,

generating a first H.323 RAS message using said first protocol, said first H.323 RAS message presenting said obtained authentication data and including an authentication request requesting authentication of the end-user by the Gatekeeper on basis of said presented authentication data,

transmitting said first H.323 RAS message to the Gatekeeper,

receiving a second H.323 RAS message from the Gatekeeper in response to said first H.323 RAS message,

interpreting said second H.323 RAS message from the Gatekeeper for detecting a confirmation or rejection of said authentication request, and

generating and sending to said end-point, on detection of said confirmation or rejection of said authentication request, an authentication confirm or reject message, respectively, using the second protocol.

16. (Previously Presented) The method of claim 15, wherein the end-point network location specification is an internet protocol (IP) address or a user name.

17. (Previously Presented) The method of claim 15, wherein obtaining the authentication data is performed by a simple html form, an applet, or a servlet.

18. (Previously Presented) The method of claim 18, wherein the applet is a signed applet.

19. (Previously Presented) The method of claim 15, wherein the second protocol includes http or https.

20. (Previously Presented) The method of claim 15, wherein the first H.323 RAS message is a H.323.V2 GRQ (Gatekeeper request) or a H.323.V2 RRQ (Registration request), respectively, including H.235 data that includes said authentication data.

21. (Previously Presented) The method of claim 15, wherein the second H.323 message is a GCF (Gatekeeper confirm) or a RCF (Registration confirm).

22. (Previously Presented) The method of claim 15, including the step of sending to the end-point of the end-user an http-response indicating authentication failure if the second H.323 message is a GRJ (Gatekeeper reject).